AMENDMENTS TO THE SPECIFICATION:

Please amend the heading beginning at page 1, line 2, as follows:

TECHNICAL FIELD ~~OF THE INVENTION~~

Please amend the paragraph beginning at page 1, line 4, as follows:

The ~~present invention generally relates~~ technology described has example application to Authentication and Key Agreement (AKA) procedures in communication systems[[,]] and ~~more particularly~~ to the use and configuration of tamper-resistant security devices in such procedures.

Please amend the heading beginning at page 1, line 8, as follows:

BACKGROUND ~~OF THE INVENTION~~

Please amend the heading beginning at page 5, line 1, as follows:

SUMMARY ~~OF THE INVENTION~~

Please amend the paragraph beginning at page 5, line 3, as follows:

The ~~present invention~~ technology described below overcomes these and other drawbacks of the prior art arrangements.

Please amend the paragraph beginning at page 5, line 6, as follows:

It is a general object ~~of the invention~~ to provide enhanced security and/or privacy in connection with authentication and/or key agreement.

Please amend the paragraph beginning at page 5, line 13, as follows:

It is also an object ~~of the invention~~ to maintain the overall security even if a tamper-resistant security device such as a SIM is used in an insecure environment or when reusing the AKA protocol over a less secure interface.

Please amend the paragraph beginning at page 5, line 20, as follows:

Still another object ~~of the invention~~ is to provide a network server supporting security and/or privacy enhancements in tamper-resistant security devices installed in user terminals.

Please amend the paragraph beginning at page 5, line 24, as follows:

As indicated above, the ~~invention generally relates~~ technology may be applied to a tamper-resistant security device, such as a subscriber identity module or equivalent, which ~~has means for storing~~ stores user credentials, including at least a security key, an AKA (Authentication and Key Agreement) module for performing an AKA process with the security key, as well as means for external communication.

Please amend the paragraph beginning at page 6, line 1, as follows:

The ~~basic idea according to a main aspect of the invention is to provide the~~ tamper-resistant security device ~~is provided~~ with an application adapted for cooperating with the AKA module, and ~~means~~ an interface for interfacing the AKA module to this application.

Please amend the paragraph beginning at page 6, line 9, as follows:

For enhanced security, the application performs somewhat different security processing tasks depending on the particular security goals to be accomplished. In general, the enhanced security processing may involve processing of one or more input parameters (pre-processing) and/or output parameters (post-processing) of the AKA process. For example, a security enhancing application may be configured for encapsulating AKA responses in a more secure algorithm, e.g. as suggested in the EAP SIM protocol mentioned above. However, ~~according to the invention,~~ all sensitive processing takes place in the tamper-resistant security device, including the security enhancing steps. Thus, considering the increased strength of the EAP SIM and similar security enhancing algorithms, the probability that attacks aimed at retrieving the secret key or other sensitive data will be successful is significantly reduced. Accordingly, the overall security can be maintained even if the tamper-resistant security device is used in a less secure environment such as a personal computer (PC), or when reusing the AKA protocol over a less secure interface such as Bluetooth.

Please amend the paragraph beginning at page 6, line 24, as follows:

Other examples of enhanced security processing that may be performed by the security application ~~of the invention~~ include i) extending the basic security functionality to generate additional keying material, e.g. one or more (possibly longer) keys based on one or more challenge-response queries,

- 5 -

ii) executing at least part of the computations required for generating a shared key for end-to-end encryption between two users (based on the key in the SIM or similar security device), and iii) masking AKA key information generated by the AKA module. For example, additional keying material could be useful for the purposes of lawful interception with increased security from the end-user's point of view, or for security enhancements associated with public access.

Please amend the paragraph beginning at page 7, line 4, as follows:

The ~~invention~~ technology can also be used to perform replay checks, ensuring that the same AKA input parameter (RAND) is not re-used in ways that are not secure. In particular, when combining several AKA output parameters into a higher security response or key, it is important to make sure that a set of unique AKA input parameters (RAND values) are used.

Please amend the paragraph beginning at page 8, line 27, as follows:

If the application files/input data are transferred into the application environment by using an existing command, such as the ENVELOPE command of the GSM SAT, the input/output interface of the tamper-resistant security device does not require any changes. This is important ~~since the invention hence~~ to ensure that the technology does not violate existing standard specifications.

Please amend the paragraph beginning at page 9, line 4, as follows:

In an alternative example embodiment ~~of the invention~~, the AKA algorithms are also at least partly implemented, preferably together with the enhanced security and/or privacy processing, as an

application in the application environment of the tamper-resistant device. ~~Apparently, this~~ This approach does not require a special interface between the resident AKA module and the application environment, since both the enhanced security and/or privacy processing and the AKA algorithms are located in the application environment. Naturally, there will still be some program code interface between the AKA algorithms and the security enhancing functionality.

Please amend the paragraph beginning at page 9, line 18, as follows:

The ~~invention~~ technology offers the following example advantages:

Please amend the paragraph beginning at page 9, line 20, as follows:

- From the terminal point of view, the ~~present invention shows how to extend~~ technology extends and ~~improve~~ improves legacy SIMs and similar tamper-resistant security devices with an extra security layer that protects the device in hostile environments subject to viruses and Trojans.

Please amend the paragraph beginning at page 9, line 28, as follows:

- ~~A main merit is that the solution~~ The technology is "future proof" and easy to administer in a secure way by authenticated downloads.

Please amend the paragraph beginning at page 10, line 1, as follows:

- The ~~solution~~ technology is in a sense transparent to the device into which the tamper-resistant security device is plugged. In addition, it enables secure remote access directly to the security device, such as a SIM, when the security device is still in the original

(mobile) terminal, communicating over e.g. Bluetooth. This means that the mobile terminal can be used as a "generic" authentication device, without threatening the security of the SIM.

Please amend the paragraph beginning at page 10, line 16, as follows:

Other advantages ~~offered by the present invention~~ will be appreciated upon reading of the below description of ~~the~~ example embodiments ~~of the invention~~.

Please delete the paragraph beginning at page 10, line 21, which starts with:

The invention, together...

Please amend the paragraph beginning at page 11, line 1, as follows:

Fig. 3   illustrates an exemplary embodiment of a tamper-resistant security device ~~according to the invention~~;

Please amend the paragraph beginning at page 11, line 4, as follows:

Fig. 4   is a schematic diagram of a user terminal equipped with a tamper-resistant security device according to an exemplary embodiment ~~of the invention~~;

Please amend the paragraph beginning at page 11, line 7, as follows:

Fig. 5   is a block diagram of an exemplary embodiment of a tamper-resistant device ~~according to the invention~~ realized as a subscriber identity module;

Please amend the paragraph beginning at page 11, line 10, as follows:

Fig. 6 is a schematic diagram of a network server supporting security and/or privacy enhancements in tamper-resistant security devices according to an exemplary embodiment ~~of the invention~~;

Please amend the paragraph beginning at page 11, line 18, as follows:

Fig. 8 is a block diagram of a further exemplary embodiment of a tamper-resistant device ~~according to the invention~~ realized as a subscriber identity module;

Please amend the paragraph beginning at page 11, line 21, as follows:

Fig. 9 is a block diagram of yet another exemplary embodiment of a tamper-resistant device ~~according to the invention~~ realized as a subscriber identity module;

Please amend the paragraph beginning at page 11, line 24, as follows:

Fig. 10 is a schematic block diagram of a tamper-resistant security device illustrating the operation of a security enhancing application according to an exemplary embodiment ~~of the present invention~~;

Please amend the paragraph beginning at page 11, line 28, as follows:

Fig. 11 is schematic block diagram of a tamper-resistant security device illustrating a security enhancing application with encapsulation and comparative pre-processing according to an exemplary embodiment ~~of the present invention~~;

Please amend the paragraph beginning at page 12, line 1, as follows:

Fig. 12 is a diagram illustrating an authentication process with privacy enhancement obtained by a tamper-resistant subscriber identity module ~~according to the invention~~; and

Please amend the paragraph beginning at page 12, line 4, as follows:

Fig. 13 is a block diagram of another exemplary embodiment of a tamper-resistant device ~~according to the invention~~ realized as a subscriber identity module.

Please amend the paragraph beginning at page 12, line 16, as follows:

~~The basic idea according to a main aspect of the invention is to provide an~~ <u>An</u> application ~~adapted for cooperating~~ <u>is provided that cooperates</u> with the AKA module ~~as well as~~ <u>and includes</u> an interface, for example an API or similar interface, between the AKA module and the application, as schematically illustrated in Fig. 3.

Please amend the paragraph beginning at page 12, line 21, as follows:

Fig. 3 illustrates an exemplary embodiment of a tamper-resistant security device ~~according to the invention~~. The security device 10 basically comprises switching logic 11, an AKA module 12, securely stored user credentials 13 including at least a security key K (possibly also user identities and pseudonyms), an application 14 adapted for cooperating with the AKA module, and a more or less direct interface between the AKA module 12 and the AKA cooperating application 14. The switching logic 11 parses commands sent to the security device and handles

communication with internal functions. The AKA module 12 comprises algorithms for authentication and/or key agreement based at least partly on the security key K.

Please amend the paragraph beginning at page 13, line 25, as follows:

The ~~invention~~ example embodiments will now mainly be presented in the context of GSM SIMs, although the ideas are also applicable to UMTS SIMs, or in fact any tamper-resistant security device having AKA functionality, and a similar application and interface as described below. Other examples include the ISIMs used for 3GPP IP multimedia, or more generally UICC cards that may contain several SIMs at the same time.

Please amend the paragraph beginning at page 15, line 7, as follows:

In a preferred example embodiment ~~of the invention~~, the AKA cooperating application 14 is implemented in the application environment provided by the SIM application toolkit, using the ENVELOPE command, or an analogous command. Input/output data to the application is then preferably also transferred into the SAT ~~by means of~~ using the ENVELOPE command.

Please amend the paragraph beginning at page 17, line 23, as follows:

As illustrated in Fig. 5, the security-device or SIM is preferably provided with the capability of checking the identity/type of the terminal or handset in which it is used. This may be performed on power-up and accomplished by the module 16, which is configured for detecting whether the SIM 10 is operated in its normal secure environment (normally the mobile) or in a less secure environment such as a PC or the like. The detection module 16 preferably controls the switching

logic 11 so that AKA ~~request~~ requests are transferred directly to the AKA module or re-routed to the application environment depending on the circumstances. This functionality could thus be utilized so that when the SIM discovers or suspects that it is not in the (correct) terminal/handset, it assumes that it is external (in an insecure environment) and enters a mode where it only accepts the SAT commands, and all requests for AKA access by resident files or commands are denied.

Please amend the paragraph beginning at page 19, line 23, as follows:

Furthermore, the terminal (mobile) may be configured to determine whether the AKA request initially comes over the normal network interface, or over another interface such as Bluetooth or IRDA (Infrared Data Association) interfaces. For example, this means that the mobile itself is capable of detecting when a request for SIM access comes over less secure interfaces, and taking appropriate actions accordingly. The origin of the request may for example be determined by the terminal based on port identification (IR Port, Bluetooth Port, Normal Radio Interface Port, etc.). Typically, instead of transferring a request for AKA processing directly to the AKA module, using the normal resident command, the AKA request is re-routed to the security enhancing application by the terminal using the SAT application environment command when the request comes over the Bluetooth or IRDA interface. This is another example of a security policy suitable for implementation ~~by the invention~~. Here also, it may be advantageous to customize the security processing by providing a number of different sub applications and selecting among the sub applications depending on the particular type of interface used by the terminal.

Please amend the paragraph beginning at page 20, line 9, as follows:

Another example of a security policy suitable for implementation in a tamper-resistant security device ~~of the invention~~ is related to the existing proposals for enhancing the security of the 3GPP Gb interface [13]. When security is in place there is also a need for policies that govern how/when to use security. Sometimes low/no security can be accepted, sometimes it cannot. Specifically, during negotiation of which security algorithms to use, there may be a problem that a man-in-the-middle performs a so-called "bidding-down attack". Suppose that the mobile terminal signals to the network that it is capable of using security algorithm "A" and "B", where "A" is much stronger than "B". If an attacker now simply deletes "A" from the list of supported algorithms, the network will believe that the mobile only supports "B" and the mobile terminal/network will end up using suboptimal security, even if both parties support also "A". For this reason, there is a suggestion to add some form of integrity protection of the negotiation. However, for some time there will be a mix of networks supporting the enhanced security negotiation, as well as some networks that have not yet been upgraded. Therefore, operators may wish to issue a policy to their subscribers, dictating if the mobile terminal should accept an insecure negotiation in a foreign, visited network. Clearly, an attractive placement for this policy control is in the application environment of a tamper-resistant security device such as a SIM. The decision as to whether insecure negotiation should be accepted is preferably based on information that is integrity protected via AKA.

Please amend the paragraph beginning at page 21, line 7, as follows:

For illustrative purposes, an example of a security policy table for implementation in a tamper-resistant security device ~~according to the invention~~ is presented below.

Please amend the paragraph beginning at page 21, line 14, as follows:

It is highly desirable to keep the SIM/ME interface intact, not affecting the standards (at least, even if new commands might need to be added, the SIMs can still be backwards compatible with the standard). It is of course also important to consider the issue of whether the terminals/handsets remain unaffected by the ~~invention~~ technology. When the SIM is to be used externally to the terminal/handset, ~~obviously~~ there is no need to change the handset, since it will not even be involved. In the case when the handset is to be used as an "authentication token" as discussed above, there is normally a need for modification. However, the mere fact that it should be possible to run GSM AKA commands over IRDA or Bluetooth alone makes modifications necessary (connecting the SIM to Bluetooth/IRDA), and ~~our invention~~ the technology regarding the SIM functionality does not make it more difficult to introduce these changes.

Please amend the paragraph beginning at page 22, line 15, as follows:

In the following, the ~~invention~~ technology will mainly be described with reference to various non-limiting examples of enhanced security processing and privacy processing implemented as software in an SAT environment of a SIM.

Please amend the paragraph beginning at page 27, line 26, as follows:

It is expected that we will soon see end-to-end (e2e) encryption between users. That is, before the conversation starts, an e2e key-agreement between the two users is performed, e.g. using the protocol MIKEY as specified in [10]. This makes lawful interception harder, since the operator must somehow be able to deduce the same key as the users obtain shared between them. The ~~invention~~ technology proposes that at least parts of the operations and computations required in connection with the e2e key-agreement are implemented as an application in a SAT-like environment, by upgrading the SIM with an application that, based on the operator-user shared key k, derives also end-to-end keys between users A and B, that "automatically" become known to the operator too.

Please amend the paragraph beginning at page 29, line 25, as follows:

This means that, based on the subscriber key, stored on the SIM, two keys must be derived, rather than just one. Moreover, k2 must not be deducible from k1. This can be accomplished by deriving k2 using the normal AKA protocol, and then $k1 = f(k2)$ for a suitable one-way function, where only this latter k1 is sent to the AP. Again, at least the generation of the further key k1 can be implemented securely as a SAT application on the SIM itself using the ~~current invention~~ technology.

Please amend the paragraph beginning at page 30, line 2, as follows:

In another aspect ~~of the invention~~, the SIM or similar security device (and more particularly the application toolkit thereof) is used to enhance the privacy of the user in a convenient way, for example by managing user pseudonyms.

Please amend the paragraph beginning at page 31, line 1, as follows:

With the present~~invention~~ technology, it is possible for the SIM, or similar security device, to store and administrate the tmpIDs, preferably in a SAT application or equivalent. When the user changes access, the SIM is connected to the new terminal (e.g. by physically moving it), thereby transferring the current tmpID (and possibly other existing security parameters) over to the new device. The new network can, preferably after having authenticated the user (involving the AKA module), now assign him a new temporary ID, tmpID'. In the somewhat simpler case that the same terminal is used but for a new session, the SIM will similarly "remember" the ID used previously and does not need to be physically moved.

Please amend the paragraph beginning at page 33, line 23, as follows:

The embodiments described above are merely given as examples, and it should be understood that the ~~present invention is~~ claims are not limited thereto. Further modifications, changes and improvements which retain the basic underlying principles disclosed and claimed herein are within the scope of the ~~invention~~ claims.